Records Management Guidance
For PKI Digital Signature Authenticated
and Secured Transaction Records

March 11, 2005

CONTENTS

List of Figures & Tables

1. Introduction

The *Records Management Guidance for Agencies Implementing Electronic Signature Technologies*, issued by the National Archives and Records Administration (NARA) on October 18, 2000, requires that Federal agencies comply with records management requirements when implementing the Government Paperwork Elimination Act (GPEA, P.L. 105-277). GPEA requires that, when practicable, agencies use electronic forms, electronic filing, and electronic signatures to conduct official business with the public by 2003.

Public key cryptography, which is used to implement digital signatures, is one of the principal electronic signature technologies that agencies use when conducting business electronically. A Public Key Infrastructure (PKI) supports the application of digital signature technology. PKI is defined as "a set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates."[1]

The goal of this document is to provide records management guidance to Federal agencies for PKI digital signature authenticated and secured[2] electronic transaction records as a supplement to

- the more general electronic signature technology records management guidance issued by NARA on October 18, 2000, entitled *Records Management Guidance for Agencies Implementing Electronic Signature Technologies* and
- the detailed guidance for PKI administrative records issued on March 14, 2003, under the title of *Records Management Guidance for PKI-Unique Administrative Records*.

This guidance document will complete the production of records management guidance necessary to ensure appropriate recordkeeping for Federal agencies employing PKI in their programs.

This guidance was initiated by the National Archives and Records Administration (NARA) and the Legal and Policy Working Group (LPWG) of the Federal Identity Credentialing Committee (FICC), which operates under the mandate of the Chief Information Officers (CIO) Council. The purpose of this detailed guidance is to assist Federal agencies in the management of PKI digital

---

[1] *Introduction to Public Key Technology and the Federal PKI Infrastructure*, National Institute of Standards and Technology, Special Publication 800-32, February 26, 2001, *http://csrc.nist.gov/publications/nistpubs/800-32/sp800-32.pdf.*

[2] The terms "authenticated" and "secured" refer to the unique capabilities of PKI digital signature technology to "authenticate" the identity of a subscriber/signer or relying party, and to "secure" or protect the integrity of the transaction content (by utilizing elements of the digital signature [the hash digest] to detect whether the bit-level content of the transaction has been compromised).

signature authenticated and secured transaction records in their normal course of conducting electronic commerce.

2. Scope

This guidance applies to Federal transaction records[3] that are authenticated and secured using PKI digital signature technology for purposes of establishing or supporting the trustworthiness of the transaction and meeting evidentiary requirements in any legal proceeding relating to the transaction.[4] PKI-related records that are created, acquired, or received as part of an electronic transaction must be stored and preserved for the retention period defined by the agency and approved by the Archivist of the United States (typically the same retention period as the transaction itself). The combination of records required to establish or support the trustworthiness of the electronic transaction is referred to in this guidance as the "Trust Documentation Set." As shown in figure 1, the records that can be part of the Trust Documentation Set fall into three categories:

1. PKI Transaction-Specific Records that are generated for each transaction. These records may be embedded or referenced within the transaction stream (e.g., the digital signature, generally the public key certificate, and possibly transaction-specific PKI records used for authentication or non-repudiation, such as certificate validation responses).

2. PKI-Unique Administrative Records that establish or support authentication, non-repudiation, and the overall trustworthiness of the electronic transaction process (e.g., the Certificate Revocation List (CRL) used to validate the subscriber/signer's certificate, subscriber agreement, documentation regarding the OCSP's operations/response, etc.)

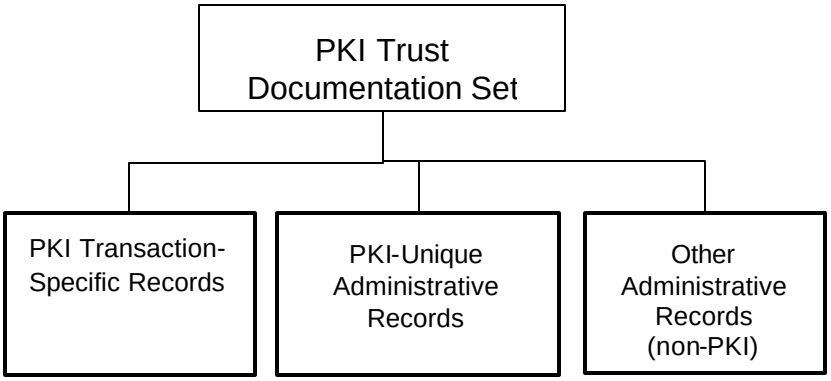
3. Other Administrative Records (non-PKI records) that can be retained and used to attest to the reliability and overall trustworthiness of the PKI-based transaction process (e.g., agency policy or agency legal counsel opinion recognizing the legal sufficiency of the PKI digital signature authentication process employed, client/browser and server setup and configuration records, application or system testing and validation records, and operational procedures and training documentation).

---

[2] The use of the term "record" throughout this guidance is as defined in the Federal Records Act 44 USC 3301 (see Glossary for definition) –
URL: ***http://www.archives.gov/about_us/basic_laws_and_authorities/disposal_of_records.html#def (for 3301***).
See also 44 USC 3101 – 3102 for a description of agency records management responsibilities –
URL ***http://www.archives.gov/about_us/basic_laws_and_authorities/federal_agencies.html#records (for 3101-3102).***

[4] Refer to the November 2000 Department of Justice publication *Legal Considerations in Designing and Implementing Electronic Process: A Guide for Federal Agencies*, which provides useful insights with regard to legal considerations. See especially sections IIB, IIC, and IIIC *(http://www.cybercrime.gov/eprocess.htm).*

Figure 1. PKI Transaction "Trust Documentation Set" Records



The target audience for this guidance includes Federal agency **information technology, information management, records management, legal department, and operations personnel** responsible for planning, implementing, operating, or otherwise documenting and managing Federal electronic transaction records that are digitally authenticated and secured using a PKI. Other entities, such as state and local government agencies, as well as commercial entities interacting with government agencies, may find this guidance document useful and may adopt and or modify it to suit their specific needs.

This guidance relates solely to the management of PKI records and is not sufficiently comprehensive to serve as a primer for understanding public key cryptography or the technical details of how a PKI functions to support digital signature authentication or how it is operated to produce, manage, and validate digital transactions. .

A high-level description of a PKI that may serve as an introduction to the technology can be found in Appendix (1) and (2) of

> *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication,* NIST Special Publication 800-25, October 2000 (see *http://csrc.nist.gov/publications/nistpubs/800-25/sp800-25.pdf)*

This guidance presumes that PKI digital signature authenticated and secured transaction records will involve disparate technology platforms and architectures that may change over time. Therefore, the guidance is designed to be technology-independent regarding any particular PKI implementation.

2.1 Out of Scope

The following areas related to PKI digital signature authenticated and secured transaction records are outside the scope of this guidance:

Transaction Content. The transaction content (whether in plain text or encrypted) to which PKI digital signature technology is applied is not within the scope of this document. However, certain PKI records may be embedded with or appended to the transaction content, such as the digital signature, the public key certificate, and other related records, and should be retained as records together with the transaction content.

Transmission of Transactions. The means or method of secure *transmission* of PKI authenticated and secured transactions is not within the scope of this document since transmission is a temporary process that does not produce records per se.

PKI Secured Transaction Records Using Encryption. Records related to the use of PKI technology for encrypting transaction content in order to protect its privacy or confidentiality is out of the scope of this guidance, except for those administrative records produced as part of Key Management Infrastructure or Services used for key management and recovery (see Section 4.8). For guidance on the privacy protection and confidentiality of PKI-based transactions (using PKI-based encryption or other means), consult with the agency's Privacy Act office and agency legal counsel.

Records Retention or Retention Schedules. Establishing a records schedule or setting retention periods for PKI transaction record Trust Documentation Sets is outside the scope of these guidelines for the following reasons:

- When retained to support the authentication of an electronic transaction content record, PKI digital signature transaction records are program records. The retention periods for program records are determined by agency business needs and then approved by the Archivist of the United States, consistent with existing NARA guidance.

- Among other considerations, the retention period for PKI digital signature transaction records will be influenced by an agency's risk assessment of the electronic transaction application and the resulting OMB-defined assurance level the agency selects.

- The retention periods established for the four assurance levels identified in the Federal Bridge Certification Authority X.509 Certificate Policy (9/27/04) relate only to Certification Authority (CA) records (PKI-Unique Administrative Records) and should be considered in the definition and approval of retention periods for electronic transaction program records.

- The retention periods for Other Administrative Records also will be influenced by the retention periods defined and approved for the electronic transaction program records.

3. PKI Transaction Process and Records

As a foundation for understanding the records management guidance for PKI transaction records, this section presents the PKI-related aspects of an electronic transaction process. It also defines the types of PKI-related records that may be created, received, acquired, or referenced by the parties involved in the transaction.

The process for each transaction typically involves the interaction of three elements:

- the subscriber/signer who configures and uses a client/browser or server that supports and executes PKI digital signature software,
- the PKI infrastructure consisting of certain agency-based or external trusted PKI services (CA, certificate repository, time stamp), and
- the relying party's (i.e., the agency's) PKI environment that authenticates and processes the subscriber/signer's transaction.

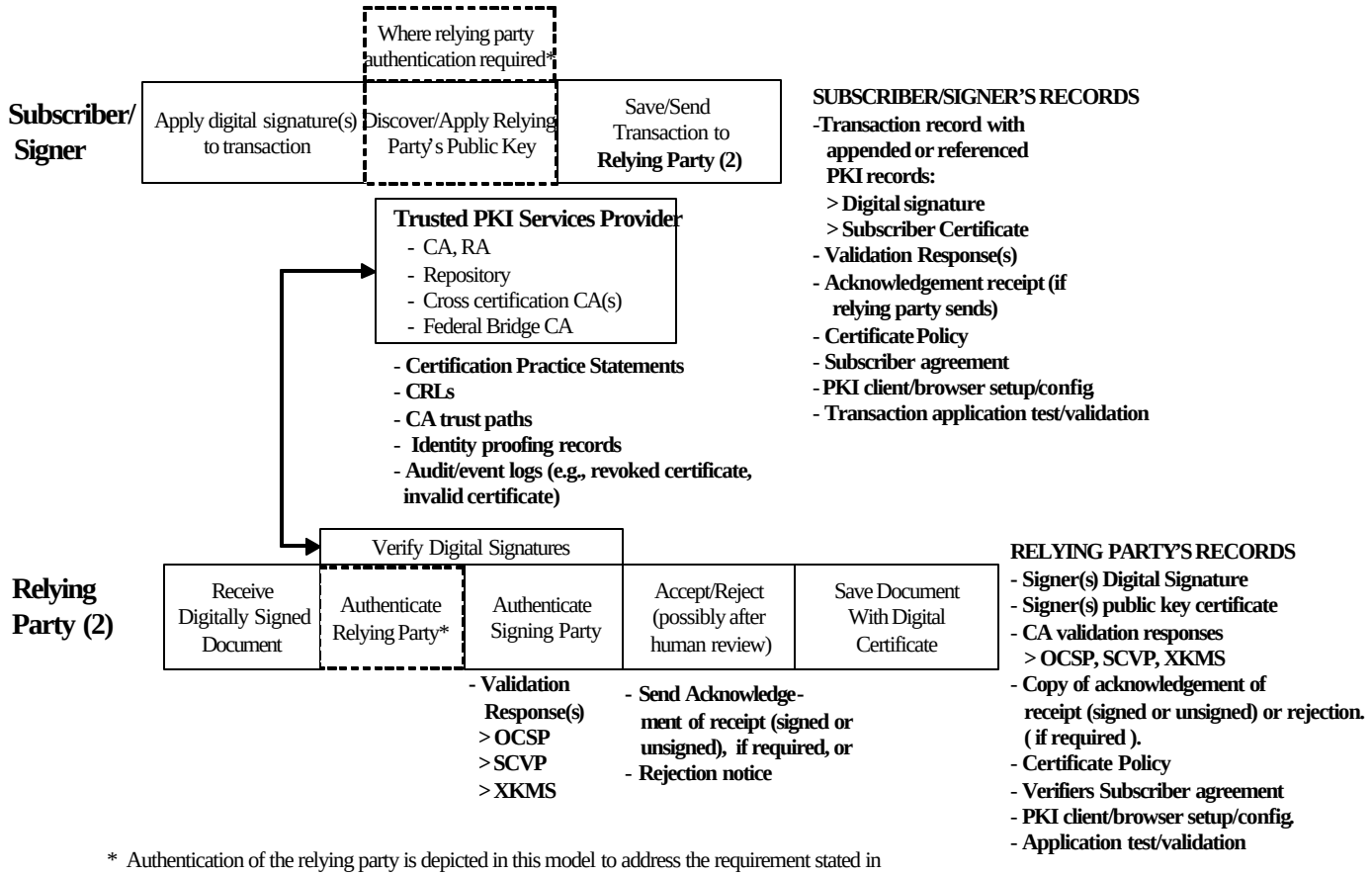
A typical PKI transaction process model is depicted in figure 2, with the example records listed at the step in the process where they may be generated, received, or maintained.

3.1 Example Process Model and Trust Documentation

Figure 2, Example PKI Transaction Process Model and Trust Documentation, depicts the process activities and example records associated with authenticating or securing a transaction using PKI digital signature technology. These typical process activities and related records are not intended to be all-inclusive since PKI transaction application implementations may differ in where and how a particular function is implemented. A more comprehensive list of example records is provided in table 3, Trust Documentation Sets by Assurance and Authentication Levels (Section 4.4). Table 3 also indicates the category of document, i.e., PKI Transaction-Specific records, PKI-Unique Administrative records, and Other Administrative records (non-PKI) as defined in section 2, Scope.

The dashed line blocks relate to the requirement for authenticating the relying party (which also must be a subscriber with a public key pair) as specified for Authentication Level 4 in the National Institute for Standards and Technology (NIST) *Electronic Authentication Guideline, Special Publication 800-63, version 1.01, September 2004.* (See section 4.6 for additional information.) The process and steps for encrypting the transaction content using PKI technology for purposes of protecting the confidentiality or privacy of the transaction during its approved retention period are outside the scope of this guidance and are not shown in Figure 2. Definitions of the terms and acronyms used in figure 2 are provided in appendix B, Glossary, and appendix C, Acronyms.

Figure 2. Example PKI Transaction Process Model and Trust Documentation
(the record examples are in **bold** type)



* Authentication of the relying party is depicted in this model to address the requirement stated in The National Institute of Standards and Technology (NIST) *Electronic Authentication Guideline, Special Publication 800-63* (June 2004), Level 4 authentication, to authenticate all parties to an electronic transaction.

4. Records Management Guidance

The objective of this detailed guidance is to help Federal agencies manage PKI digital signature authenticated and secured transaction records. The recommendations and requirements stated in this guidance draw upon existing records management, regulations, standards, guidance, and best practices.

The areas addressed in this records management guidance are derived primarily from the following activities and research:

- An initial information-gathering activity, including two focus group sessions with participants from multiple Federal agencies on May 12 and 13, 2004. These two sessions identified potential areas and issues for consideration when developing records management guidance for Federal PKI digital signature transactions. A number of the areas and issues the focus groups identified have been incorporated into this guidance.

- Review of recent PKI-related guidance and reference documentation, including guidance and informational documents from OMB, NARA, NIST, DOJ and Request for Comment (RFC) documentation from the Internet Engineering Task Force (IETF) and World Wide Web Consortium (W3C) (see Appendix A for detailed reference information).

- Various discussions with selected Government agencies and PKI infrastructure software vendors.

This records management guidance applies to the three categories of Federal records identified in section 2, Scope:

1. PKI Transaction-Specific records that may be embedded or referenced within each transaction (e.g., the digital signature, generally the public key certificate, and possibly transaction-specific PKI records used for authentication or non-repudiation, such as certificate validation responses).

2. PKI-Unique Administrative records, which are generally retained separate from the transaction data, support authentication, non-repudiation, and the overall trustworthiness of the electronic transaction process (e.g., certificate validation responses, the CRL used to validate the subscriber/signer's certificate, subscriber agreement, etc.)

3. Other Administrative records (non-PKI records) that can be retained and used to attest to the reliability and overall trustworthiness of the PKI-based transaction process, such as client/browser and server setup and configuration records, application or system testing and validation records, and operational procedures and training documentation.

The following records management principles underlie the keeping of Federal records that comprise the Trust Documentation Set for PKI digital signature authenticated and secured transactions.

4.1 Recordkeeping Principles

All Federal PKI digital signature authenticated and secured transaction records should:

- Contain the human-readable name of the subscriber/signer. This could be the Subject name from the public key certificate or other metadata that represents the name of the subscriber/signer.
- Include a human-readable date and time associated with the signing of the transaction that is "at or near the time"[5] that the signing occurred.
- Indicate the intent of the subscriber/signer, i.e., the purpose for applying the PKI digital signature to the transaction. The intent may be obvious if it relates directly to a purpose included in the text of the transaction, e.g., "approved by" or "submitted by." It could be in the form of a statement that the subscriber/signer takes responsibility for the transaction or that the subscriber/signer is authorized to sign on behalf of someone else. It also may relate to the context of the transaction (e.g., a purchase order form).

For the PKI-related transaction records, the operational or recordkeeping system should:

- Capture all PKI transaction records that meet the definition of a Federal record. Also, the metadata needed for identification, searching and disposition management of the transaction should be captured "at or near the time" of the transaction.
- Retain PKI recordkeeping Trust Documentation Sets for at least the same period of time as the digitally signed transaction to which they pertain.
- Avoid the retention of PKI transaction records on any individual user's workstation because
  - integrity protection is not automatically provided and is limited to user-modifiable file controls (e.g., a reversible read-only setting),
  - accessibility is limited to the user(s) who has access to the files on the workstation, and
  - disposition management cannot be programmatically controlled.

[5] Federal Rules of Evidence 803(6) - a "[r]ecord of a regularly conducted activity" such as a "memorandum, report, record, or data compilation, in any form" will be admissible if the record was made "at or near the time by . . ."

4.2 Recordkeeping Responsibility

Each Government agency is responsible for the lifecycle management of all records that are part of the defined Trust Documentation Set for each PKI-based digitally signed electronic transaction. The agency should capture and preserve these records for the approved retention period, after which temporary records may be destroyed and permanent records transferred to NARA.

The agency should not assume that PKI transaction records will be retained for the approved retention period by any third party unless specific legally binding and enforceable agreements have been made for retention. Even when such legally binding and enforceable agreements are in place, periodic reviews should be conducted to ensure adherence by the trusted third party. It is recommended that agencies maintain control of key PKI authentication records, such as identity proofing documentation and subscriber agreements, where possible.

Where an agency agrees to rely on a credential issued by another agency, the relying agency should ensure both (1) that it has a legally binding and enforceable agreement with the agency that issued the credential under which the issuing agency sets forth its retention policies and agrees to make materials available as needed, and (2) that any legally binding and enforceable agreements with third parties make clear which materials must be retained for, and made available to, the relying agency.

Therefore, both the subscriber/signer and relying parties as well as the trusted PKI service provider(s) – either the agency(ies) or third party(ies) under a legally binding and enforceable agreement – have recordkeeping responsibilities. They should ensure that all records of the PKI Trust Documentation Set related to each PKI digitally signed electronic transaction are retained for the required period of time as defined in and approved for a particular program or application

The following are examples of approaches that may be used to ensure that the records are properly retained.

- The subscriber/signer and relying party may generate or acquire all records, including records from pertinent trusted PKI services provider(s), and retain them for the required period of time in a manner that meets recordkeeping requirements. This can be done either under control of the operational transaction environment (e.g., database) or as transferred to and under control of a recordkeeping system.

- The subscriber/signer and relying party may enter into a legally binding and enforceable agreement with one or more trusted third-party PKI service providers to retain certain records, such as CRLs or subscriber agreements, for the required period of time in a manner that meets good recordkeeping requirements.

For PKI transaction records that are retained physically separate from the transaction but are referenced or linked from within the transaction data stream, the following records management requirements should be met.

- The integrity and quality of the reference or the link to the PKI transaction record from within the transaction data stream should be maintained for the approved retention period of the record. Separating transaction-specific PKI-related records from the transaction data stream is not recommended, except where the usability of the transaction content by a downstream application or reproduction tool may be restricted.

- All records should be managed in accordance with good recordkeeping guidance, whether they are managed within an operational transaction system or a recordkeeping system.

4.3 PKI-Unique Administrative and Other Administrative Records as Trust Documentation

Administrative records, which play a very important role in the overall Trust Documentation Set for PKI transaction records, are of two types:

- PKI-Unique Administrative records that are not part of the PKI transaction stream but may be referenced either from within the PKI-portion of the transaction stream or may reside as separate records that are related to the transaction. Examples of these records are:

  - certificate validation responses that may be retained either physically and logically separated from PKI transactions or together with the transaction data,

  - the CRL used to validate the subscriber/signer's certificate,

  - the subscriber agreement, and

  - event or audit logs for revoked certificates or negative certificate validation responses, etc.

- Other Administrative records that are not specifically related to the PKI can play an important role in attesting to the reliability and overall trustworthiness of the PKI transaction process. Examples of these records are

  - client/browser and server setup and configuration records that may drive the number and sequence of PKI events,

  - transaction application or system testing and validation records, and

  - operational procedures and training documentation for the PKI infrastructure and the transaction application.

It should be noted that certain administrative records that do not relate specifically to an individual subscriber/signer, such as the Certificate Policy, the browser setup/configuration, and other training and operating procedure documentation, need only be retained once at the agency or transaction information system level and not by each individual subscriber/signer.

PKI-Unique Administrative and Other Administrative Records may play a substantial role in providing additional evidence that supports the authentication of the parties to the transaction and strengthens non-repudiation. These records also provide support for the reliability and trustworthiness of the entire PKI-based transaction application.

The importance of retaining administrative records increases with the selected level of identity assurance and authentication requirements (as defined in OMB Memorandum M-04-04[6] and NIST Special Publication 800-63[7] and discussed in more detail later). This is especially the case where the selected assurance level and technical authentication level (such as OMB and NIST Levels 3 and 4 and possibly Level 2) may require additional proof for authentication and non-repudiation.

For supporting authentication of the Signer, records such as certificate validation using a CRL or a validation response protocol may be required. For supporting non-repudiation, a subscriber agreement or the public key certificate may contain information regarding the signature authority of the subscriber/signer(s). If PKI functions and processes related to the transaction application are questioned, then supporting system or program documentation records, such as the application specification, client/browser PKI setup or configuration, or PKI testing and validation documentation may be required to provide proof of trustworthy system operation.

One of the strongest roles of Other Administrative Records is documenting how a PKI process and the transaction application function on a regular basis in the normal course of business. These records include

- operating procedures,
- user and administrator training documentation,
- client/browser and server PKI setup and configuration that drive the sequence of PKI digital signing events, and
- testing and validation documentation for the PKI elements of the transaction application.

---

[6] Office of Management and Budget – OMB Memorandum M-04-04 E-Authentication Guidance for Federal Agencies, December 16, 2003, http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf.

[7] National Institute of Standards and Technology – NIST Special Publication 800-63, June 2004 for Electronic Authentication. http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63v6_3_3.pdf

These records can provide a strong foundation for establishing the regular operation of the PKI transaction application in the normal course of business. For the lower assurance and authentication levels (OMB and NIST levels 1 and 2), these supporting records may provide sufficient trust documentation to alleviate the need for retaining the digital signature and other embedded PKI transaction record documentation, assuming the authentication of the digital signature and the integrity validation of the transaction content have been properly executed.

Given the relative novelty of PKI technology and the untested nature of PKI digital signature transaction processes in the courts, the following two recommendations can strengthen the legal sufficiency of the PKI-based transaction information system and each transaction.

- For each PKI-based transaction information system, establish an agency policy, procedure or legal counsel opinion[8] that establishes the legal sufficiency of the PKI digital signature authentication process employed. This policy, procedure, or legal opinion would describe in business and legal terms, versus more complex PKI-related terminology, the processes, methods, and technology employed in the regular course of business to ensure that each PKI-based transaction is executed and recorded in an accurate and reliable manner. Since this policy, procedure, or opinion could be released to the public or a court or oversight body, it should not contain privileged legal analysis, discussions of risk assessment, or other sensitive materials.

- For each transaction, the application should automatically (where possible) create a textual, easily understood "summary trust record." The purpose of this record is to provide proof, in layman terminology rather than PKI-technical terminology, to a court or other interested parties that the PKI-based transaction process complied with agency policy and procedure. This summary trust record should collect, at a minimum, the fact that the PKI digital signature is valid, the date/time validated, and the transaction ID. Other information recommended for inclusion in the record is a specific reference to the policy, procedure, or legal counsel opinion record noted above (including the date and version of the record), and any other pertinent information deemed necessary to establish legal sufficiency based on the agency's risk assessment.

4.4 Linking of PKI Records to Assurance and Authentication Levels

The type and number of PKI digitally signed transaction records that may need to be retained to establish trustworthiness over time will be influenced by the selected assurance level that results from the agency's risk assessment. This section discusses how the assurance levels set forth by OMB and the authentication processes set forth by NIST for electronic transactions may influence the type and amount of PKI transaction records that should be retained and managed.

---

[8] Office of Management and Budget, Implementation of the Government Paperwork Elimination Act, (May 2, 2000) Section 8. How should agencies implement electronic signatures and electronic transactions? "a. Build from a policy framework. GPEA applies to interactions between outside entities and the Federal government, as well as to transactions and record keeping required by parties under Federal programs. Accordingly, agencies should consider whether their policies or programmatic regulations support the use and enforceability of electronic signature alternatives . . ."

OMB issued the *Memorandum on E-Authentication Guidance for Federal Agencies* on December 16, 2003 (M-04-04). This memorandum identified four assurance levels that are based on the confidence level that is required regarding the validity of the asserted identity of the electronic signature applied to a transaction. NIST issued the *Electronic Authentication Guideline, Special Publication 800-63,* as technical guidance supplementing the OMB M-04-04 E-Authentication Guidance.

Table 1, Summary of Assurance Levels and Technical Authentication Guidance, presents a summary of the OMB assurance level and NIST authentication level guidance. This summary is provided as background regarding both the potential applicability of PKI at each assurance level and as a baseline for determining the records that may need to be retained as part of the Trust Documentation Set for PKI digital signature authenticated and secured electronic transactions.

Table 1. Summary of Assurance Levels and Technical Authentication Guidance

Identity Assurance Level	OMB M-04-04 E-Authentication Guidance (required confidence level)	NIST 800-63 Electronic Authentication Guideline (electronic authentication requirements)	PKI Applicability
1	Little or no confidence in the asserted identity's validity	No identity proofing is required at this level. Although an authentication mechanism provides some assurance that the same claimant is accessing the protected transaction, there is not a requirement at this level to use FIPS-approved cryptographic techniques.	Optional
2	Some confidence in the asserted identity's validity.	Authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token. Level 2 requires identity proofing but does not require FIPS-approved cryptography. It allows any of the token methods of levels 3 and 4, as well as passwords and PINs.	Yes
3	High confidence in the asserted identity's validity.	Level 3 authentication requires cryptographic strength mechanisms that protect the primary authentication token against compromise. Relying parties must determine which data requires authentication or confidentiality protection and are not required to authenticate or encrypt all data transferred. Authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token.	Yes
4	Very high confidence in the asserted identity's validity.	Requires strong cryptographic authentication of all parties and all sensitive data transfers between parties. Strong, FIPS-approved cryptographic techniques are used for all operations.	Yes

The four assurance levels (Rudimentary, Basic, Medium, and High) identified in X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA)[9] essentially map to the four OMB assurance levels and the four NIST levels of authentication where PKI technology is used to authenticate and secure the transaction content, as indicated in table 2.

Table 2. Summary of FBCA Assurance Levels Relative to OMB and NIST

X.509 Certificate Policy, Federal Bridge Certification Authority Assurance Levels	OMB M-04-04 E-Authentication Guidance (required confidence level)	NIST 800-63 Electronic Authentication Guideline (electronic authentication requirements)
Rudimentary	1	1
Basic	2	2
Medium	3	3
High	4	4

4.4.1 PKI Trust Documentation Sets by Assurance and Authentication Levels

Table 3, Trust Documentation Sets by Assurance and Authentication Levels, provides guidance regarding which PKI transaction records should be retained in order to provide the appropriate level of reliability, authenticity, integrity, usability, and non-repudiation relative to the four assurance levels as defined in OMB Memorandum M-04-04 and the signature authentication guidance described in NIST's *Electronic Authentication Guideline, Special Publication 800-63* (September 2004).

The possible records to be retained are listed by the three entities involved in a PKI-based transaction environment – namely, the Signer, the Relying Party, and Trusted PKI Services Providers. A discussion of each of the four Trust Documentation Sets, including the rationale for recommending that certain records be retained, follows the table.

[9] X.509 Certificate Policy for the Federal Bridge Certification Authority, *http://www.cio.gov/fpkipa/documents/FBCA-CP.pdf.*

The recommendations provided in table 3 are for guidance only. The actual records that need to be retained and the authentication methods required to be employed may vary based on the risk assessment conducted by the agency, including the risk of future litigation. Due to the relative newness of PKI technology, both from an implementation and a litigation perspective, it is recommended that agencies err on the side of inclusiveness when determining which PKI transaction records should be retained, especially for assurance levels 2, 3, and 4. Once business and legal experience has been gained, the decision regarding which specific PKI-related transaction records should be retained can be revisited.

The column in table 3, labeled "Category" relates to the categories of records that are defined in section 2, Scope. Entries in the cells for this column are abbreviated as

TS = PKI Transaction-Specific records

UA = PKI-Unique Administrative records

OA = Other Administrative records (non-PKI records)

Entries in the cells under the four columns labeled "Level n" are abbreviated as

O = *Optional*: The record is not necessarily required to support the trustworthiness of the transaction, but agencies should assess the risk associated with the transaction to determine whether retention is appropriate.

R = *Recommended*: The record would support the trustworthiness of the transaction; however, its retention should be evaluated based on the overall Trust Documentation Set being retained and for the risk of legal or regulatory action and the potential consequences of the action.

SR = *Strongly Recommended*: The record should be retained to support the trustworthiness of the transaction.

Table 3. Trust Documentation Sets by Assurance and Authentication Levels

Example Trust Documentation Records	Cate-gory	Level 1	Level 2	Level 3	Level 4
Subscriber/Signer[10]					
Digital Signature	TS	O	SR	SR	SR
Public key certificate	TS	O	SR	SR	SR
Certificate Validation Response(s) – OCSP, XKMS, SCVP (for relying party's public key certificate, and possibly for the CA(s) that authenticated the certificate.	TS	O	O	R	SR
Time Stamp (where applicable)	TS	O	O	R	SR
Acknowledgement of Receipt (where provided by the Relying Party)	TS	O	O	R	SR
Subscriber Agreement (through Registration Authority)	UA	O	R	SR	SR
Certificate Policy (including signature and/or role authority where applicable)	UA	O	R	SR	SR
Agency policy or agency legal counsel opinion establishing the legal sufficiency of the PKI digital signature authentication process employed	OA	O	R	SR	SR
PKI configuration or setup of Signer's application	OA	O	O	R	R

[10] The example records listed under the Subscriber/Signer, Relying Party and Trusted PKI Service Provider are records that may be created, received, or acquired and retained by that party. In the case of a Certificate Policy, it needs to be retained only by the Subscriber or Relying Party's organization, not by each individual. More than one party may choose to retain a specific record, such as a relying party acquiring and retaining a CRL, which also would be retained by the Trusted PKI Service Provider (although possibly for a shorter period of time than the Relying Party requires).

Example Trust Documentation Records	Cate-gory	Level 1	Level 2	Level 3	Level 4
client/browser and/or server					
PKI-specific documentation related to the electronic transaction application (e.g., requirements, specifications, setup, test or validation plan and results, etc.)	OA	O	O	R	R
Relying Party					
Signer's Digital Signature (enveloped with or referenced from transaction)	TS	O	SR	SR	SR
Signer's Public Certificate (enveloped with or referenced from transaction)	TS	O	SR	SR	SR
Signer's Certificate Validation Responses – OCSP, XKMS, SCVP	TS	O	R	SR	SR
Acknowledgment receipts (record copy of what was sent to Originator/Signer)	TS	O	O	R	SR
Time Stamping (where applicable)	TS	O	O	R	SR
Textual "summary trust record" for each transaction documenting that the PKI digital signature is valid, the date/time, and the transaction ID, plus any other information deemed necessary from the agencies risk assessment.	TS	O	R	SR	SR
Certificate Revocation List (from trusted PKI services provider)	UA	O	O	R	SR
Audit event log for invalid certificates or invalid hash comparisons	UA	O	O	R	R

Example Trust Documentation Records	Cate-gory	Level 1	Level 2	Level 3	Level 4
Agency policy, procedure, or legal counsel opinion establishing the legal sufficiency of the PKI digital signature authentication process employed,	OA	O	R	SR	SR
PKI-related configuration/Setup of Client/Browser and/or Server	OA	O	O	R	R
PKI-related documentation related to the electronic transaction application (e.g., requirements, specifications, setup, test or validation plan and results, etc.)	OA	O	O	R	R
Trusted PKI Services Provider (either agency or third party administered)					
Certification Practices Statement (for CA or validation services)	UA	O	R	SR	SR
Certificate Revocation Lists (CA or Repository)	UA	O	O	R	SR
Time Stamping	TS	O	O	R	R
Identity proofing records (RA)	UA	O	R	SR	SR
Audit event logs: for revoked certificates, etc. (CA or Repository), or invalid validation responses (CA or Repository)	UA	O	O	R	SR

Level 1: Trust Documentation Set

For a level 1 assurance environment, no PKI records may need to be retained because the one-time acts or processes of verifying the digital signature against a public key certificate (verifying the validity date range), then verifying the integrity of the transaction content, may suffice for validating the subscriber/signer's identity and the integrity of the transaction. Level 1 assurance does not require the use of cryptographic techniques but does suggest employing an authentication mechanism that provides some assurance that the same claimant is accessing the PKI digital signature authenticated and secured transaction.

Level 2: Trust Documentation Set

Level 2 does not require FIPS-approved cryptographic means for authenticating the signing/sending party. However, when PKI-based authentication is employed, it is recommended that the level 2 Trust Documentation Set include retention of the digital signature, the public key certificate, the identify proofing documentation, the subscriber agreement, and the certificate validation response that relate to each transaction, plus the certificate policy and the certification practices statement.

Level 3: Trust Documentation Set

Level 3 incorporates the trust documentation suggested for Level 2, but it also requires stronger authentication and non-repudiation documentation. One way to achieve stronger authentication and non-repudiation is to require relying parties to transmit a proof of receipt that is retained with the Trust Documentation Set. Where knowledge of the precise time of the digital signing is required, a time stamp should be generated and retained. Additionally, it is suggested that the agency retain certain PKI-Unique Administrative records, such as the CRL and the subscriber agreement, as well as Other Administrative records, such as the browser and server configuration and setup documentation and the system testing and validation results for the transaction information system.

Level 4: Trust Documentation Set

At level 4, which requires cryptographic authentication of all parties and all sensitive data transfers between parties, there may be a need to retain extensive records (in addition to those identified in Level 3), for providing

- proof that both parties to the transaction were authenticated and that the full trust chains supporting the public key certificates were verified via certificate validation responses, and
- additional non-repudiation documentation, such as a time stamp and acknowledge of receipt records.

4.5 Requirements Definition and Implementation Planning

Information Systems (IS)[11], including those that agencies use to implement PKI-based electronic transaction applications, will produce new records or augment existing records. A critical first step in several of the system development stages is the identification, definition, development, and refinement of the data model that includes treatment of the PKI-based digital signature transaction records that will be created and should be managed.

It is very important that all PKI-related digital signature transaction records deemed necessary to meet the requirements for reliability, authenticity, integrity, and usability are identified, defined, and integrated into the records management strategy for the PKI-based information systems or transaction applications. **Information technology, records management, legal counsel, and the business owners of the records should work closely together to completely and accurately identify all PKI-related transaction records (along with other records related to the transaction information system) and develop appropriate retention schedules and management requirements.**

At a minimum, the following is recommended:

- The requirements definition and development process for an electronic transaction information system or application should include the identification, definition, and implementation of records management functionality for PKI-based transaction records and associated metadata.

- The overall data model for a PKI-based electronic transaction information system or application should address the requirements for managing all PKI-related records, both those that are integral to the transaction data stream as well as PKI-unique administrative and other administrative supporting records. This may include the acquisition of certain records from trusted PKI services and maintenance of the referential integrity of links to certain records that are stored at trusted PKI services repositories.

- Implementation of the PKI transaction records management strategy should include defining and implementing the means to automatically capture as many of the identified records as possible, thereby reducing or eliminating the need for manual intervention by users or records management personnel.

- Where the life cycle of the PKI-related records exceeds the life cycle of the transaction application system—

    - Develop a strategy and means for migrating the PKI-based records to a recordkeeping system or to a replacement information or application system as part of the definition and planning for the original transaction information system or application.

---

[11] Information System is defined as "a discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual." Office of Management and Budget, Circular No. A-130, Revised (Transmittal Letter No. 4)

- Develop a records schedule for either the transactional information system or individual transactions, considering PKI-based records. This would include, upon finalization of the schedule, specification of terms and conditions of transfer for any records deemed of permanent value to NARA. For those records, develop a plan that would include defining a means for accomplishing such transfers at the appropriate time in the life of the records in a NARA-accepted file format.

- Agencies should also consider whether the significance of PKI transaction records will be comprehensible as a practical matter after the end of the life cycle of the information system that generated them. This may require instituting procedures and implementing processes to ensure that the records remain human-accessible and readable, either by retaining system documentation (or the system itself) or by generating and/or migrating all necessary information.

4.6 Digital Signature Detached from the Transaction Record

The concept of digital signatures being physically "detached" or separated from the transaction or document content is described in the NIST's *Common Format for Information that is Digitally Signed: A Final Report* and the W3C's Proposed Recommendation, *XML Signature Syntax and Processing.*[12] The NIST report recommends retaining the signature separately in those cases where the application that created or originated the record is not able to apply a digital signature or where the relying party's application would not be able to properly render a digitally signed version of the document.

For detached or physically separate digital signatures, a link or reference (a uniform resource identifier [URI] or transform in the case of XML[13]) should be embedded in the transaction data stream and the integrity of this reference or link maintained for the approved retention period of the transaction record at the same or higher level of assurance as the electronic transaction program requires for risk mitigation.

The recordkeeping challenge is to ensure that the digital signature and related records are accessible and can be presented in a human readable format when required.

Due to this challenge, the recommendation is to embed or append the digital signature and other directly associated information (e.g., the digital certificate) as an integral part of the transaction data stream, unless the signature needs to be retained separately in order for the transaction to be signed by the sending party's application or in order for it to be made usable by the relying party's application.

---

[12] The following references identify various formats for digitally signing electronic documents: 1) "Common Format for Information that is Digitally Signed: A Final Report", NIST, November 2001, http://csrc.nist.gov/pki/signed_info_format/welcome.htm; and 2) "XML Signature Syntax and Processing", W3C Proposed Recommendation, August 20, 2001: http://www.w3.org/TR/2001/PR-xmldsig-core-20010820/.

[13] Ibid.

4.7 Longer-Term Retention and Revalidation of Digital Signatures

Revalidation of a digital signature after the public key certificate has expired (typically 12 to 36 months) faces several major hurdles, including:

- The CRLs that were in effect during the validity range of the certificate may no longer be available (unless contractually assured between the verifying party and the relevant trusted PKI services provider),
- Over a longer period of time (typically 8 to 10 years) technology obsolescence may have resulted in replacement of the original PKI transaction program application and associated IT infrastructure (hardware and software), and
- If the PKI transaction records need to be migrated to a new format, it is likely that the underlying bit stream will change so revalidation will produce a different digital signature hash value that will no longer match the hash value generated at the time of the initial signing.

Since litigation will typically occur after the expiration of a public key certificate, it is important to take steps to ensure that pertinent records remain available after the certificate has expired. It is equally important that they be complete and understandable without the need for technical interpretation, to the extent possible.

There are options other than revalidation that can satisfy long-term authentication concerns. One option is to use digital time stamping—either internal to the agency or a third party service. The digital time stamp attests that the transaction, content and associated digital signature existed at a specific point in time.[14] The initial time stamp should be applied "at or near the time" the digital signature was applied to the transaction and the time should be derived from a trusted timeserver. Depending on the duration of the retention period and the technological duration of the time stamp technology, additional time stamps may need to be applied periodically to assure the continued trustworthiness of the records.

A second option would be to re-sign the records periodically using a trusted private key, especially during media renewal or migration, and thereby establish a digital chain of authentication.[15] Of course, this option presumes that the initial digital signature was correctly authenticated.

---

[14] See Request for Comment (RFC) 3126, *Electronic Signature Formats for long term electronic signatures*, September 2001; http://www.apps.ietf.org/rfc/rfc3126.html

[15] Please consult the DoJ Guidance (http://www.cybercrime.gov/gpea.htm or http://www.cybercrime.gov/eprocess.htm) and consult with your agency's general counsel.

4.8 Key Management Infrastructure Records

As stated in section 2.1, Out of Scope, encryption of transaction content per se is outside the scope of this guidance. However, certain PKI-related records may need to be managed over time as part of a key management infrastructure employed to facilitate the recovery of the private key used by a subscriber/signer for encrypting the transaction content to protect its confidentiality or privacy. As part of key management, the PKI key materials (e.g., a user's private encryption key) are backed up and retained by a CA or a key recovery agent.[16]

Where transaction records are retained over longer periods of time that are individually encrypted or contain individually encrypted portions, key management can become a significant recordkeeping burden due to the potential volume of encryption keys that may need to be retained and the complexities of executing key recovery and managing the resulting records, especially those keys relating to the subscriber. For these reasons, storing plain text of individual transactions is generally preferable to storing encrypted text. From a records management records perspective, where information is required to be stored in encrypted form over a longer period of time, bulk encrypted repositories offer a more easily managed alternative.

Where an agency employs PKI for encrypting the transaction content and the agency keeps transaction records in the form of individually encrypted text, provisions should be made for the retention of sufficient PKI-based records, including PKI-Unique Administrative and Other Administrative records, to facilitate key recovery and provide proof of any resulting events related to the recovery, such as the request for key recovery, issuance of a new key, etc. Key recovery records should be maintained at a level of trustworthiness that is commensurate with the assurance level of the PKI credentials (e.g., the retention of Level 2 key recovery records should meet Level 2 assurance and authentication requirements).

4.9 NARA Requirements for Permanent Electronically Signed Records

Section 5.6 of NARA guidance entitled *Records Management Guidance for Agencies Implementing Electronic Signature Technologies*, October 18, 2000, states that: "For permanent records, agencies must ensure that the printed name of the electronic signer, as well as the date when the signature was executed, be included as part of any human readable form (such as electronic display or printout) of the electronic record." NARA requires this so that the name of the signer and the date of signing will be preserved as part of the record. Therefore, all electronic transaction records, including PKI authenticated and secured transaction records, that are to be transferred to NARA for permanent retention must meet these minimum requirements.

For digitally signed records that have been scheduled and appraised as permanent, NARA currently has no intention of using the digital signature's re-validation capabilities to establish

[16] For more information on key management infrastructures and key recovery, see Section 8.1 Key Management Infrastructure/Public Key Infrastructure (KMI/PKI) at the following URL: http://www.iatf.net/framework_docs/version-3_1/index.cfm

authenticity of the record or of maintaining that capability into the future. NARA currently lacks an infrastructure to support key escrow necessary to maintain digital signature re-validation capabilities. Furthermore, agencies would attest to the authenticity and integrity of the record at the time of transfer of legal custody of the materials to NARA. Finally, based on experience with secondary users of archival records, embedded handwritten ("wet") signatures hold limited value for research. NARA presumes that this use paradigm will continue to apply. It is unlikely that PKI-related records establishing the trust of a particular transaction would be scheduled and appraised as permanent.

4.10 Metadata

For business operations, business or regulatory audit, and legal discovery purposes, there may be a need to retrieve the PKI transaction trust documentation related to a specific transaction or set of transactions.

The PKI records that are an integral part of the transaction data stream (e.g., digital signature and public key certificate) should be accessible for viewing in conjunction with the transaction data. Also, PKI records that are referenced or linked from within the transaction data stream should also be viewable in conjunction with the transaction content (this assumes that the quality and integrity of the references or links has been maintained).

For records kept physically separate from the transaction data stream (i.e., not embedded or referenced within the transaction), metadata should be automatically acquired, where possible, and stored in a database separate from the records. This would particularly apply to certain PKI-unique administrative records, such as a CRL or CPS where they are acquired and retained separately by the agency, or to supporting records such as the setup and configuration records of the PKI-enabled client/browser or application server.

The following metadata is recommended by category of record:

- For PKI records embedded with or referenced within the transaction data stream and for most PKI-unique administrative records related to each transaction (e.g., CRL, Certificate Policy, CPS), the following metadata should be automatically acquired, where possible, and retained in a database separately from, but linked to the records:
    - Certificate Policy (CP) Object Identification (OID)
    - Serial Number of subscriber/signer(s)'s public key certificate (and the relying party's public key certificate if used for authentication purposes).
    - Date and time of signing
    - Common or Distinguished Name
- For Other Administrative (non- PKI) records, such as the PKI setup and configuration of client/browser interface or application server, testing and validation records, and user or administrator procedures and training records, the following metadata is recommended:

- Program, project, and/or application name
- Certificate Policy Object ID

4.11 Multiple Digital Signatures on PKI Transaction Records

There are two key considerations with regard to multiple digital signatures on PKI digital signature authenticated and secured transactions. The first involves a policy decision of whether multiple digital signatures represent co-signing (in which case each signature is independent of the other signatures) or counter-signing (in which case each digital signature signs the transaction, as well as the signatures that precede it). The second key issue occurs when the PKI-based transaction records are very large and the operational system will not support the transmission as a single digitally signed PKI transaction.[17] In this situation, the question is whether each segment of the document should be individually signed.

When selecting the appropriate agency methodology for dealing with multiple digital signatures, consider the following.

- Seek the advice of agency legal counsel for clarification regarding the intended use of multiple PKI digital signatures, and then use the clarification to guide implementation.
- The agency's digital signature policy should stipulate whether a digital signature represents co-signing or counter-signing. The consequences of applying the digital signature should be made clear to the subscriber/signer at the time of signing.
- If the transaction is transmitted in segments due to its size, the following options may apply.
  - If only one segment is digitally signed, the signature properties box should state that the signer(s) take responsibility for the remaining linked segments.
  - Digitally sign each segment of the transmission, and ensure that the segments are linked to logically represent a single transaction and provide assurance of the integrity of the combined segments.

[17] For example, the Nuclear Regulatory Commission (NRC) requires PKI digitally signed transaction documents for certain regulatory submissions. Many of these documents are quite voluminous and involve as many as six or seven signatures. Currently, the NRC cannot support transmissions that exceed 50 MB. Hence, the current NRC practice is to digitally sign the first segment and reference the remaining segments.

4.12 PKI Transaction Records Stored in Databases

Transaction records and their associated PKI records that are stored in databases should be retained as historical records, either as separate, protected records within the database or transferred to appropriate storage media from which the records can be recovered and reloaded for viewing and reproduction as required.

The databases should have the ability to meet the requirements of the records management guidance for Operational Systems as stated in Section 4.13, Detailed Records Management Guidance below.

4.13 Detailed Records Management Guidance

PKI digital signature transaction records are similar in nature to other electronic and hard copy records, including PKI-unique administrative records. Therefore, they do not require the creation of separate or distinct records management requirements or guidance. Recordkeeping requirements based on relevant laws, regulations, standards, and best practices should be applied to PKI digital signature transaction records just as they are applied to other agency records.

The recordkeeping guidance as stated in the *Records Management Guidance for PKI-Unique Administrative Records* issued by NARA in March 2003, with the exception of the metadata area as discussed in section 4.10 above, covers all of the records management requirements that relate to PKI-unique administrative records and can be directly applied to all PKI digital signature transaction records identified in this guidance document.

Therefore, the records management guidance provided in section 5 of the *Records Management Guidance for PKI-Unique Administrative Records* is incorporated by reference into this guidance document –
http://www.archives.gov/records_management/pdf/final_pki_guidance.pdf.

The *Records Management Guidance for PKI-Unique Administrative Records* covers requirements for two types of systems for managing PKI records: 1) *operational systems*, which typically are database applications that include the PKI-based transaction application and PKI-unique administrative application(s), and 2) *recordkeeping systems*, applications specifically designed to manage, preserve, and provide access to records for the approved retention period. The recordkeeping system may also include placing and releasing legal holds on the records and managing the migration of records as required due to technology or application obsolescence. Each agency should configure and operate each system to meet specified records management requirements.

The records management guidance provided in section 5 of the *Records Management Guidance for PKI-Unique Administrative Records* is drawn from the following sources:

- NARA "Records Management Guidance for Agencies Implementing Electronic Signature Technologies"
- NARA 36 CFR 1234 Regulations
- DoD 5015.2 Standard, Version 2

- ISO 15489, Parts 1 and 2
- FBCA X.509 Certificate Policy for the FBCA (Note: at the time these guidelines were developed, the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework did not exist)
- GSA ACES Certificate Policy
- Good practice

Table 4 lists the detailed records management guidance areas that are covered in the *Records Management Guidance for PKI-Unique Administrative Record.*

Table 4. Overview of Records Management Guidance Areas

Guidance Area	Operational System	Recordkeeping System
Record Capture	X[18]	X
Record Metadata	X	X
Record Classification		X
Record Retrieval	X	X
Record Disposition	X	X
Record Integrity	X	X
Record History Log		X
Records Storage	X	X
Vital Records	X	
Records Audit Trail	X	
Records Privacy	X	X
Record Security	X	X
Record Freezes/Holds	X	X
Record Transfer to a Recordkeeping System	X	
Long-Term Retention	X	X
Record Preservation		X

[18] An "X" in the column indicates that this area is covered in the *Records Management Guidance for PKI-Unique Administrative Records.*

Appendix A. References and Sources

The following references and sources were used as the basis for producing the list of PKI-specific records and the depiction of the PKI-related transaction process:

- Access Certificates for Electronic Services (ACES), Certificate Policy http://www.gsa.gov/Portal/gsa/ep/contentView.do?programId=10064&channelId=-13479&ooid=9577&contentId=8647&pageTypeId=8199&contentType=GSA_BASIC&programPage=%2Fep%2Fprogram%2FgsaBasic.jsp&P=9FG3

- Common Format for Information that is Digitally Signed: A Final Report, NIST, November 1, 2001 http://csrc.nist.gov/pki/signed_info_format/welcome.htm

- NIST Special Publication 800-63 Electronic Authentication Guideline http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63v6_3_3.pdf.

- Office of Management and Budget - OMB M-04-04 E-Authentication Guidance for Federal Agencies, December 16, 2003 http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf

- PKI Basics – A Technical Perspective, PKI Forum, November 2000 http://www.pkiforum.org/pdfs/PKI_Basics-A_technical_perspective.pdf.

- Records Management Guidance for Agencies Implementing Electronic Signature Technologies (NARA), October 18, 2000 http://www.archives.gov/records_management/policy_and_guidance/electronic_signature_technology.html.

- Records Management Guidance for PKI-Unique Administrative Records, NARA, March 2003, http://www.archives.gov/records_management/pdf/final_pki_guidance.pdf.

- X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework http://www.cio.gov/ficc/documents/CommonPolicy.pdf.

- FBCA X.509 Certificate Policy for the FBCA http://www.cio.gov/fpkipa/documents/fbca_cp_09-10-02.pdf

Appendix B. Glossary

These definitions are derived from a variety of sources, including the NARA **Records Management Guidance for Agencies Implementing Electronic Signature Technologies**, DoD 5015.2, X.509 PKIX, X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA), and glossaries in several books relating to PKI and digital signatures.

Acknowledgement of receipt. Office of Management and Budget, Implementation of the Government Paperwork Elimination Act (May 2, 2000), Section 8. How should agencies implement electronic signatures and electronic transactions? Consider providing an acknowledgment of receipt. The agency's system for receiving electronic transactions may be required by statute to have a mechanism for acknowledging receipt of transactions received and acknowledging confirmation of transactions sent, with specific indication of the party with whom the agency is dealing.

Certification Authority. A trusted organization that can accept certificate applications from subscribers, issues digital certificates, and either maintains status information about certificates or arranges for a trusted third party to perform these services. Note: In some cases, a Certificate Authority (CA) may be defined in a more narrow sense, such as "The CA is collection of computer hardware, software and the people who operate it" (Housley and Polk, p. 44).

Certificate Policy. A written document that identifies the applicability of a class of certificates with common security requirements and sets forth the requirements that are appropriate for applications or uses. Public Key Infrastructure (X.509) has created an outline and guidance for the content of certificate policy documents.

Certification Practices Statement. A written document that articulates the practices that a Certification Authority employs in issuing, managing, revoking, and renewing certificates. Public Key Infrastructure (X.509) has created an outline and guidance for the content of certificate practice statements.

Certificate Revocation List. This is a Certificate Authority's listing of unexpired certificates that cannot be trusted (i.e., revoked certificates).

Certificate Validation. The process of authenticating that a public key certificate is valid at a specific point in time. Typical methods and protocols used for validation are: CRL, OCSP, SCVP, XKMS (see Acronyms).

Classification. The systematic identification and arrangement of business activities and/or records into categories according to logically structured conventions, methods, and procedural rules represented in a classification scheme that meets the specific business needs of the agency. A PKI classification scheme could be designed that defines records, record files or folders, records subseries, and records series for each of the primary PKI administrative functions.

Common Name. The given name of an individual or organization that corresponds to its real world identity.

Content. The information that a record is meant to convey which may consist of words, phrases, numbers, symbols, etc. (see PKI Transaction Record)

Context. The organizational, functional, and operational circumstances in which documents are created and/or received and used. Also, the placement of records within a larger records classification system providing cross-references to other related records.

Cross Certificate. A certificate used to establish a trust relationship between two Certification Authorities.

Digital Signature. The result of a transformation of a message by means of a cryptographic system using keys such that a Relying Party can determine: (1) whether the transformation was created using the private key that corresponds to the public key in the subscriber/signer's digital certificate; and (2) whether the message has been altered since the transformation was made.

Disposition. Actions taken regarding records after they are no longer required to conduct current Agency business.

Distinguished Name. A unique name or character string for each individual in a CA directory that unambiguously identifies each subscriber.

Electronic Signature. Per Section 1710. Definitions of Title XVII – Government Paperwork Elimination Act (GPEA, P.L. 105-277).

> (1) ELECTRONIC SIGNATURE.—The term "electronic signature" means a method of signing an electronic message that—
>
> > (A) identifies and authenticates a particular person as the source of the electronic message; and
> >
> > (B) indicates such person's approval of the information contained in the electronic message.

Federal Record. The Federal Records Act - 44 USC 3301 defines a record as:

"… all books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them. Library and museum material made or acquired and preserved solely for reference or exhibition purposes, extra copies of documents preserved only for convenience of reference, and stocks of publications and of processed documents are not included."

Freeze. The suspension or extension of the disposition of temporary records that cannot be destroyed on schedule because of special circumstances, such as a court order or an investigation.

Good Practice. Good practice indicates that no specific regulatory or other official standard or framework can be cited, yet where the guidance point is very important to ensure proper management of records for the approved retention period. The good practice guidance cited in this document is derived from various records management studies and reports and from knowledge and experience derived from the application of records management practices in commercial and public entities.

Individual Subscriber. A subscriber is an individual who has generated a private/public key pair and has been issued a digital certificate after being appropriately identified and authenticated as part of a registration process.

Information System. "A discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual." Office of Management and Budget, Circular No. A-130, Revised (Transmittal Letter No. 4)

Integrity. The integrity of a record refers to its being complete and unaltered over time.

Legal and Financial Rights Records. (See Vital Records.)

Logical PKI Record. A logical PKI record consists of data content stored in relational database tables or other proprietary or raw data format that exists as a physical record only at the time of rendering for viewing, printing, or saving. If the rendered physical record is not printed or saved, then it ceases to exist as a physical entity. If the data content has not changed, then a specific logical record can be retrieved and accurately rendered innumerable times. As an example, the data representing the content of a digital certificate may exist in two or more database tables, but the digital certificate exists as a physical entity only at the time that the data content is retrieved and used to populate a digital certificate template. This digital certificate may then be printed or saved as a physical entity.

Metadata. Data describing stored data, that is, data describing the structure, content, and context, and other characteristics of electronic records. Record profile data.

Object ID. A unique identifier for a Certificate Policy that is registered with the American National Standards Institute so that a certificate issuer and a certificate users (subscriber) can both recognize and reference the policy.

Operational System. The software and hardware system that performs the day-to-day activities of running and maintaining a PKI, such as a CA or the actual software that is creating and/or executing the electronic transaction. In an operational system, the active content (such as public key certificate data elements) and event information (audit log) typically are stored in relational database tables. Since this content or event data may be the official and possibly the only source of this information for a period of time, the operational system can be said to contain the "record

file copy" of that information. While the data may be backed up for disaster recovery purposes, operational systems typically do not provide the functionality that is necessary to effectively manage records disposition or other traditional records management functions.

PKI-Unique Administrative Record. PKI records that are created, used, maintained, and preserved to support ongoing management and operation. They do not include subscriber transactions in which a public key has been used for signing or for another purpose.

PKI Secured Transaction Record. A transaction in which the integrity of the content can be secured or protected using public key cryptography by utilizing elements of the digital signature (the hash digest) to detect whether the bit-level content of the transaction has been compromised.

PKI Transaction Record. A record that is created by the actual use of a public key certificate to digitally sign an electronic document or consummate an electronic commerce transaction.

PKI Trust Documentation Set. Records that may be part of the Trust Documentation Set fall into three categories:

1. PKI-unique transaction embedded records related specifically to each transaction and that are embedded or referenced within the transaction (e.g., the digital signature, generally the public key certificate and possibly transaction-specific PKI records used for authentication or non-repudiation, such as certificate validation responses).

2. PKI-unique administrative records that support authentication, non-repudiation and the overall trustworthiness of the electronic transaction process (e.g., certificate validation responses, the CRL used to validate the subscriber/signer's certificate, subscriber agreement, key generation process documentation, etc.)

3. Other administrative records (non-PKI records) that can be retained and used to attest to the reliability and overall trustworthiness of the PKI-based transaction process, such as client/browser and server setup and configuration records, application or system testing and validation records, and operational procedures and training documentation.

Records that fall into the trust documentation set will vary from agency to agency based on assessments of risk. There is no "one size fits all" solution. Furthermore, the level of detail in what is retained will vary from transaction to transaction.

Record. (See Federal Record.)

Record File Copy. A "record file copy" is the final or "official" copy that is retained according to a NARA-approved retention schedule. (See Federal Record.)

Recordkeeping System. A manual or automated system in which records are collected, organized, and categorized to facilitate their preservation, retrieval, use, and disposition for the approved retention period.

Registration Authority. An entity that is responsible for identification and authentication of certificate subjects prior to the issuance of certificates, but which does not sign or issue certificates (i.e., a Registration Authority is delegated certain tasks on behalf of an authorized CA).

Registration Authority. A person or agency who has received information that includes a certificate and a digital signature verifiable with reference to a public key listed in the certificate and is in a position to rely on them.

Relying Party. The recipient of a certificate and a digital signature verifiable with reference to a public key listed in the certificate and who is in a position to rely on them or a person who otherwise relies on the binding in a certificate between the public key appearing in it and the identity (and/or other attributes) of the person named in the certificate.

Repository. A system or collection of distributed systems that store certificates and CRLs and serves as a means of distributing these certificates and CRLs to end entities.

Retention Period. The period defined by the agency and approved by the Archivist of the United States that records must be kept before they are destroyed or transferred to NARA. Records approved for transfer to NARA by the Archivist of the United States have a retention period of "permanent." A retention period is sometimes referred to as " approved retention" because NARA has approved the disposition of the records.

Structure. The physical and logical format of a record and the relationships between the data elements.

Subscriber (Signer). A subscriber is an entity that (1) is the subject named or identified in a certificate issued to that entity, (2) holds a private key that corresponds to the public key listed in the certificate, and (3) does not itself issue certificates to another party. This includes, but is not limited to, an individual or network device

Trusted PKI Services Provider. A general term used in this guidance document to describe essentially all potential providers of trusted PKI services, which could be either agency-administered or provided by a trusted third party, such as a registration authority, certification authority, repository, time stamping service, etc.

Vital Records. Essential records that are needed to meet operational responsibilities under national security emergencies or other emergency or disaster conditions (emergency operating records) or to protect the legal and financial rights of the Government and those affected by Government activities (legal and financial rights records). Emergency operating records are the type of vital records essential to the continued functioning or reconstitution of an organization during and after an emergency. (A vital record may be both an emergency operating record and a financial rights record.)

Appendix C. Acronyms

ACES. Access Certificates for Electronic Services (General Services Administration)

CA. Certification Authority

CFR. Code of Federal Regulations

CP. Certificate Policy

CPS. Certification Practice Statement

CRL. Certificate Revocation List

IETF. Internet Engineering Task Force

FICC. Federal Identity Credentialing Committee

FIPS. Federal Information Processing Standard

FBCA. Federal Bridge Certification Authority

LPWG. Legal and Policy Working Group of the Federal Identity Credentialing Committee

OCSP. On-line Certificate Status Protocol

OID. Object Identifier

PKIX. Public Key Infrastructure (X.509) (Internet Engineering Task Force Working Group)

RA. Registration Authority

SCVP. Simple Certificate Validation Protocol

URI. Uniform Resource Identifier

W3C. World Wide Web Consortium

XML. Extensible Markup Language

XKMS. XML Key Management Services